EUROPEUM
Brussels Office

December
2021

Policy Paper

Challenges of regulating innovative technologies

Michala Stupková

Ministry of Foreign Affairs
of the Czech Republic

The project was supported by the Ministry of Foreign Affairs of the Czech Republic in the framework of public diplomacy projects within Czech foreign policy and international relations

EUROPEUM Brussels Office

December 2021

Contents

Summary

Modern technologies are an inherent part of today's world and research is advancing at a rapid pace. The disruptive technologies such as AI, DLT, IoT, VR or robotics are currently booming for instance in healthcare, transportation, agriculture, energetics, or finance. Although the use of these innovative technologies undoubtedly provides many benefits to various subjects, it might also potentially pose certain risks. Regulators all over the world are therefore challenged to find the most efficient regulatory approaches that would not only achieve the intended regulatory objectives but also wouldn't result in unnecessary administrative barriers or in prevention of a further development of innovations. Some of the obstacles the regulators face are, however, the rapidly changing environment, the length of the legislative process or limited understanding of the technology. This policy paper therefore identifies the regulatory challenges and demonstrates a few legislative techniques used by the European union in the recent legislative proposals which aim to tackle these challenges. Furthermore, the policy paper summarizes the key principles that the EU should adhere to when regulating new technologies to ensure the appropriate protection of users, businesses, investments, or financial stability while at the same time supporting technological innovation. Robust but reasonable regulation without unnecessary and overly burdensome obligations seems to be the solution for the EU to be a global regulatory standard setter and to stay at the forefront of the tech development.

Ministry of Foreign Affairs of the Czech Republic

The project was supported by the Ministry of Foreign Affairs of the Czech Republic in the framework of public diplomacy projects within Czech foreign policy and international relations

EUROPEUM Brussels Office

December 2021

Challenges of regulating innovative technologies

Regional The new emerging technologies that are sometimes also being called disruptive technologies (since they have the potential to disrupt the current status quo and change the markets completely) are an essential part of today's world, society, and almost every sector of the economy, where they help with automatization and optimization of processes. The digital transformation, a widely used buzzword meaning integration of digital technology into all areas of a business resulting in fundamental changes to how businesses operate and how they deliver value to customers, is a trend that has been at the forefront for many years now. Business from all sectors, as well as the public sphere, are incorporating technologies in their daily operations, so their use is becoming ever more widespread. Sectors in which the use of technology is currently booming are for example healthcare, transportation, agriculture, energetics, or finance.

As the new emerging technologies are most often considered artificial intelligence ("AI"), virtual and augmented reality ("VR" and "AR"), distributed ledger technology ("DLT"), Internet of things ("IoT"), robotics, or biometric technologies. Although the use of these technologies undoubtedly offers many benefits to various subjects, it might also, in some cases, pose certain risks. The most common benefits are understood to be a more comprehensive offer of new products or services, promotion of competition and the resulting reduction in prices and improvement in product quality. On the other hand, the potential risks are mostly connected to privacy issues (for example unauthorized misuse of personal data), profiling, or possible bias or inexplicability of AI outputs.

There is no doubt that, as well as in other areas, the potential risks must be addressed by proper legislative frameworks. The European approach might be different from other approaches by being probably more protective and more ex-ante oriented. However, the bottom line is almost always that the technology should not be regulated right after its emergence. Firstly, it should be observed how the systems and applications based on this technology work or are being used, and whether some potential risks should be addressed. Subjecting the at-risk systems or applications under the regulation, setting rules for their use, and enabling supervisory agencies to control and enforce compliance with those rules, can thus ensure adequate protection for protected interests and entities. Nonetheless, the million-dollar question is, what is the most effective way to do so and whether to focus on providing a general framework, a "playground" that defines rather key principles and objectives or to impose strict and specific rules.

The European Union clearly stated digitalization and innovation support as its priority and has been very active in this area. The European Commission continuously monitors new technological developments and publishes in this field various analyses, public consultations, or strategies. To mention some of the notable ones: A Europe fit for the digital age 2020 -2024, European data strategy, Digital finance package, Shaping Europe's digital future or Europe's digital decade: digital targets for 2030. The strategies are in principle followed by legislative proposals. The most discussed and ground-breaking legislative proposals in this regard are, for example proposal for a Regulation laying down harmonized rules on artificial intelligence (AI Act), proposal for a Regulation on Markets in Crypto-assets, and amending Directive (MiCA), proposal for a Regulation on a pilot regime for market infrastructures based on distributed ledger technology (DLT pilot regime) or proposal for Regulation on digital operational resilience for the financial sector (DORA). The Commission has also published a number of legislative proposals in another related area – data governance – for example a proposal for a Regulation on European data governance (Data Governance Act - DGA) that should govern secure and trusted data sharing or proposal for Regulation on contestable and fair markets in the digital sector (Digital Markets Act - DGM) ensuring a fair environment for online platforms and social networks and a proposal of Regulation on a Single Market For Digital Services (Digital Services Act – DSA) adapting commercial

Ministry of Foreign Affairs of the Czech Republic

The project was supported by the Ministry of Foreign Affairs of the Czech Republic in the framework of public diplomacy projects within Czech foreign policy and international relations

and civil law rules for commercial entities operating online. The Commission also plans to publish a Data Act by the end of 2021, facilitating data access and use and reviewing the rules on databases' legal protection.

Regulating innovative technologies, however, brings a specific set of challenges. As a new area of law is emerging and developing – the IT law or law of new technologies – there are not many guidelines or examples of good practice on tackling these challenges. The regulators must deal with the underlying principle that the development will always be way ahead of the legislatures and the legislative process. The legislative process takes several months up to years, during which time technologies usually change and evolve, and their new applications arise. Therefore, it is very challenging to create a future-proof regulation that might be able to stand alone for many years after enactment. Another issue associated with the previous one is that it is almost impossible for the legislators or the supervisory authorities to have deep and up-to-date knowledge and understanding of the functioning of every single technological application. Not only do the public bodies lack the insight into these applications and systems, but it is also in many cases not possible to create standard rules such as technical operational standards or requirements for all various applications because there is no typical regulatory model or use case.

Due to the reason mentioned above, the so-called "performative or performance-based rules or regulation"[1] is being used more and more when regulating new technologies. The performative rules are, in comparison to the usual legal rules less rigid and more inflexible. When using the performative regulation, the legislator requires the regulated entity to determine the specific rules that will ensure achieving the desired outcome and objectives set by the legislation. That means a clear description of the possible risks and clear descriptions of how each risk has been addressed. The idea behind it is that the regulated entity knows best what needs to be done to achieve the purpose of the regulation in the most effective way. The content of the "internal regulation" is therefore left to the discretion of the regulated subject based on the specific parameters of the respective system or network. That means individual entities implement completely different rules, but they lead to the same goal. The supervisory role is then to supervise whether the measures are sufficient and whether they are being adhered to. In this case, the relationship between the law and the regulated entity is similar to the relationship between the law and the public authority tasked with implementing the law in the form of a by-law.

This approach can be viewed as a form of "co-legislation." Some performative rules were used by the European legislators for example in the NIS directive[2] or in GDPR[3]. The performative rules in the GDPR for example require for the controller to know (and document) what personal data they process, why and how they process it, what the security risks are, and to set out their own obligations to protect the personal data. Therefore, the controller is obliged to ensure that the processing of personal data is carried out in accordance with data protection legislation, taking into account its nature and the risks it poses. The controller also needs to demonstrate compliance with these rules, which is subsequently assessed by the supervisory authority, with the burden of proof resting on the data controller. In the event of a personal data breach, the controller is obliged to report the breach to the competent authorities.

[1] This term frequently appears in publications of doc. Radim Polčák such as: Polčák, R., Kasl, F., Loutocký, P., Míšek, J. and Stupka, V., 2019. *Virtualizace právních vztahů a nové regulatorní metody v pozitivním právu*. Právník, [online] (1). Available at: <https://www.ilaw.cas.cz/casopisy-a-knihy/casopisy/casopis-pravnik/hledat-v-archivu/detail-clanku.html?id=44655&r=%252Fcasopisy-a-knihy%252Fcasopisy%252Fcasopis-pravnik%252Fhledat-v-archivu.html%253Fnaki_search%253D1%2526form_state%253D%2526query%253Dinte> [Accessed 7 November 2021].

[2] Directive (EU) 2016/1148 of the European Parliament and of the Council of 6 July 2016 concerning measures for a high common level of security of network and information systems across the Union (further referred to as „NIS directive")

[3] Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation) (further referred to as the „GDPR")

Ministry of Foreign Affairs of the Czech Republic

The project was supported by the Ministry of Foreign Affairs of the Czech Republic in the framework of public diplomacy projects within Czech foreign policy and international relations

Another interesting approach of the EU is not to regulate the technology itself but the potential high risk or prohibited applications. The technology itself is not the problem, but some of its applications may cause risks to natural persons' health and safety, fundamental rights, or other interests and values protected by law. Some applications can even be considered unacceptable as contravening Union values, for instance, by violating fundamental rights. Moreover, in some cases it would not even be possible to regulate the technology itself. For example the decentralized technologies, which in its essence do not have any central administrator that oversees the operational processes or has the power to make changes and could be therefore held accountable, unless they get somehow 'recentralized' by determining one accountable party. The solution to balance the total absence of a central controlling and full supervision seems to be to regulate the providers of the services or perhaps the developers of the protocol or other incentivized parties.

Lastly, harmonization is essential when designing a regulation of new technologies. National borders are less important in today's globalized world, moreover, in the digital world, where they are almost non-existent. The individual national regulations make it more difficult for businesses to scale up to different non-harmonized markets. As a result, this can hamper innovative European companies compared to other global players, e.g. from the US or China, where a product can be immediately launched in markets of hundreds of millions.

Current significant initiatives in technological regulation

AI Act

European Commission introduced this new regulatory framework on AI in April 2021. The AI Act aims to harmonize the rules of using AI systems by providing a horizontal legislative act that should ensure trustworthy, transparent, and human-centric AI. Before publishing the proposal, Commission assessed four different policy options [4] of the regulatory intervention. The possible approaches were for example just voluntary scheme, a sectoral "ad-hoc" approach, or different variants of horizontal EU legislative instrument. The approach that Commission chose in the end was to create a horizontal EU legislative instrument following a proportionate risk-based approach and the voluntary codes of conduct for non-high-risk AI systems. The Commission opted for a horizontal approach based on the assumption that a sectoral approach would be very lengthy and challenging as many individual acts would have to be discussed and negotiated. That could result in rules and obligations in individual acts being very fragmented and inconsistent, making it much more complicated for the concerned entities to navigate the regulation and search through several regulations to find which rules apply to them. Nevertheless, some sectoral regulations may emerge, for example, on autonomous vehicles, but it is expected that these acts will somehow refer to the AI Act. The AI Act does not regulate the technology itself but only the AI systems that can adversely affect fundamental rights from the EU Charter of Fundamental Rights.

The proposal, therefore, distinguishes four levels of risks with a different set of rules for each level. The first level is the prohibited artificial intelligence practices that would contravene EU values, cause physical or psychological harm to a person, or exploit any of the vulnerabilities of a specific group of persons. These are for instance social scoring or remote facial recognition. One level lower are the high-risk AI systems, which are various AI systems listed in Annex III that can adversely impact people's safety or their fundamental rights. Those are, among others, AI systems intended to be used for recruitment or selection of natural persons, AI systems intended to be used by law enforcement authorities for predicting the occurrence or reoccurrence of an actual or potential criminal

[4] Chapter 3. 3. of the Explanatory memorandum of the Proposal for a regulation of the European Parliament and of the Council laying down harmonised rules on artificial intelligence (Artificial Intelligence Act) and amending certain Union legislative acts (COM (2021) 206) (further referred to as the "AI Act")

Ministry of Foreign Affairs of the Czech Republic

The project was supported by the Ministry of Foreign Affairs of the Czech Republic in the framework of public diplomacy projects within Czech foreign policy and international relations

offense based on profiling of natural persons or AI systems intended to be used to evaluate the creditworthiness of natural persons or establish their credit score. The two lowest levels are the AI systems that represent limited or minimal risk. Deep fakes, chatbots, or emotion recognition systems would belong to the level with limited risk and would therefore be subjected to a limited set of obligations, e.g. transparency[5]. The minimal risk AI systems are being encouraged by the AI Act to draw up a "*codes of conduct intended to foster the voluntary application to AI systems of requirements related for example to environmental sustainability, accessibility for persons with a disability, stakeholders participation in the design and development of the AI systems and diversity of development teams on the basis of clear objectives and key performance indicators to measure the achievement of those objectives.*[6]". Other AI systems can be developed and used in the EU without any additional legal obligations than the existing legislation.

When drafting the proposal, Commission decided on some interesting legislative approaches. One of these not-so-common legislative techniques, which may be a bit controversial, was not to put the definition of the technology in the text of the regulation but in the annex [7]. The intention was to ensure that the definition could be changed more flexibly, only by the delegated act of the Commission instead of by the proper legislative process. That might be one way to solve the problem of defining an ever-evolving technology and ensure that the regulation remains future-proof and reflects the development. Some, however, view that the Commission gives itself too much power by allowing itself to change the scope of the regulation. However, if the Commission were to change the definition of AI by a delegated act, e.g. add or remove a technique from the list in Annex II, it would have to submit an explanatory memorandum. In addition, once the Commission adopts the act, Parliament and Council generally have two months to formulate any objections. If they do not, the delegated act enters into force. Another interesting approach concerning the definition is that instead of one complex definition of AI, the technology is defined by listed techniques and approaches in Annex II[8].

Furthermore, the regulation in AI Act tends to shift more to the so-called "ex-ante" regulation, which means that the rules for the AI systems are set "from the beginning" solely on the basis that they might cause risks. For example, AI Act sets out requirements for ex-ante conformity assessments to establish that high-risk AI systems meet these requirements before they can be offered on the market or put into service. It does not give a chance to the system to "prove itself." This approach towards AI is unique since most global jurisdictions gravitate instead towards ex-post regulation. The ex-post regulation is being imposed retrospectively to address conduct on the market, which has already occurred like individual decisions of the regulators on sanctions or dispute settlements. That means to only deal with the AI systems when an issue arises and only on a case-by-case basis. It can be argued that this approach does not provide adequate legal certainty for the providers of such AI systems or that the safety of the users cannot be guaranteed. Either way, it burdens the providers less with compliance and related costs and enables them to deploy products on the market much easier and, therefore, support further innovation development.

To tackle the issue with more considerable administrative and financial barriers to deploy products on the market, the AI Act entails in Title V measures that should make it easier, especially for

[5] *Providers shall ensure that AI systems intended to interact with natural persons are designed and developed in such a way that natural persons are informed that they are interacting with an AI system, unless this is obvious from the circumstances and the context of use*"). Article 52 of the AI Act

[6] Article 69, section 2 of the AI Act

[7] Article 3, section 1 of the AI Act and Annex I of the AI Act

[8] More specifically the Artificial Intelligence is defined as: *(a)Machine learning approaches, including supervised, unsupervised and reinforcement learning, using a wide variety of methods including deep learning; (b)Logic- and knowledge-based approaches, including knowledge representation, inductive (logic) programming, knowledge bases, inference and deductive engines, (symbolic) reasoning and expert systems; (c)Statistical approaches, Bayesian estimation, search and optimization methods.*
Source: Annex I of the AI Act

Ministry of Foreign Affairs of the Czech Republic

The project was supported by the Ministry of Foreign Affairs of the Czech Republic in the framework of public diplomacy projects within Czech foreign policy and international relations

the SMEs. The first one are AI regulatory sandboxes, which should establish a controlled environment to test innovative technologies for a limited time based on a testing plan agreed with the competent authorities. „*The objectives of the regulatory sandboxes should be to foster AI innovation by establishing a controlled experimentation and testing environment in the development and pre-marketing phase with a view to ensuring compliance of the innovative AI systems with this Regulation and other relevant Union and Member States legislation; to enhance legal certainty for innovators and the competent authorities' oversight and understanding of the opportunities, emerging risks and the impacts of AI use, and to accelerate access to markets, including by removing barriers for small and medium enterprises (SMEs) and start-ups*[9]." Title V also contains measures to reduce the regulatory burden on SMEs and start-ups such as that Member state should provide small-scale providers and start-ups with priority access to the AI regulatory sandboxes, organize specific awareness-raising activities about the application of this regulation or establish a dedicated channel for communication with small-scale providers and user and other innovators to provide guidance and respond to queries about the implementation of this regulation[10]. Whether those measures are sufficient and would be truly effective in reducing the regulatory burden, we shall see.

The regulation of AI in the USA

In comparison to the European harmonized horizontal regulation, the USA, known as the world tech leader, decided for a different approach. Currently, there is no complex and horizontal federal act in force in the USA that would regulate AI. The most significant activity in this regard on federal level is that in 2019, following an Executive Order on Maintaining American Leadership in Artificial Intelligence[11], the White House's Office of Science and Technology Policy released a draft Guidance for Regulation of Artificial Intelligence Applications[12], which includes ten principles for United States agencies when deciding whether and how to regulate AI.

However, the principle of impact assessment of the AI system, meaning setting out the foreseeable unintended outcomes and sources of risks of each AI system, along with a risk-management plan designed to address such risks „ *should be familiar to U.S. lawmakers — it aligns with the impact assessments required in a bill proposed in 2019 in both chambers of Congress called the Algorithmic Accountability Act. Although the bill languished on both floors, the proposal would have mandated similar reviews of the costs and benefits of AI systems related to AI risks. That bill that continues to enjoy broad support in both the research and policy communities to this day, and Senator Ron Wyden (D-Oregon), one of its cosponsors, reportedly plans to reintroduce the bill in the coming months."*[13]

In terms of the state level, some legislative initiatives (mostly bills or resolutions, some pending, some enacted) can be found in certain states.[14] Those are focused mainly on issues connected to data privacy or unfair discrimination. Some of the AI systems are regulated in specific sectors like autonomous

[9] Recital 72 of the AI Act
[10] Article 55 of the AI Act
[11] Federal Register. 2019. *Maintaining American Leadership in Artificial Intelligence*. [online] Available at: <https://www.federalregister.gov/documents/2019/02/14/2019-02544/maintaining-american-leadership-in-artificial-intelligence> [Accessed 7 November 2021].
[12] Vought, R., 2020. *MEMORANDUM FOR THE HEADS OF EXECUTIVE DEPARTMENTS AND AGENCIES*. [ebook] Washington: Executive Office of the President. Available at: <https://www.whitehouse.gov/wp-content/uploads/2020/11/M-21-06.pdf> [Accessed 7 November 2021].
[13] Burt, A., 2021. *New AI Regulations Are Coming. Is Your Organization Ready?*. [online] Harvard Business Review. Available at: <https://hbr.org/2021/04/new-ai-regulations-are-coming-is-your-organization-ready> [Accessed 7 November 2021].
[14] Ncsl.org. 2021. *Legislation Related to Artificial Intelligence*. [online] Available at: <https://www.ncsl.org/research/telecommunications-and-information-technology/2020-legislation-related-to-artificial-intelligence.aspx?fbclid=IwAR1jhFrhl0refXSo60mSbiurB_S375DoWfJdcl8eB-4Z92FNFK5y1etbaa4> [Accessed 7 November 2021].

Ministry of Foreign Affairs of the Czech Republic

The project was supported by the Ministry of Foreign Affairs of the Czech Republic in the framework of public diplomacy projects within Czech foreign policy and international relations

cars [15] or facial recognition. Another example of existing regulation would be the Artificial Intelligence Video Interview Act (820 ILCS 42) enacted by the Illinois General Assembly[16]. The act provides that employers must notify applicants before a videotaped interview that artificial intelligence may be used to analyse the interview and consider the applicant's fitness for the position. Employers must also provide each applicant with information before the interview explaining how the artificial intelligence works and what general types of characteristics it uses to evaluate applicants and obtain a consent from the applicant to be evaluated by the artificial intelligence program.

Some states decided to use "soft-law" guidelines on implementing trustworthy AI in some sectors instead of "hard regulation". For example, New Jersey introduces guidelines for creditworthiness determinations [17] concerning affordable housing programs. The guidelines are also introduced by supervisors in their respective fields, for example Federal trade commission published guidelines[18] for companies that use AI. In its guidance[19] they advise that the use of AI tools should be transparent, explainable, fair, and empirically sound while fostering accountability. In many states, specific AI commissions or working groups are being established to monitor the use of AI and prepare guidelines in specific sectors to ensure transparent, fair, and responsible AI. Some states also focus their efforts on ensuring the transparent use of AI in government decision-making or other state services.

MiCA

Since the use of distributed ledger technology is growing and represents new opportunities as well as risks for the financial industry, the European Commission published a proposal of a Regulation on Markets in crypto-assets ("MiCA"). MiCA is intended to allow EU consumers and investors to safely access new investment opportunities or new types of payment instruments, competing with existing ones to deliver fast, cheap, and efficient payments, in particular for cross-border, without the risk of fraud, money laundering, or illegal practices in crypto-asset markets. The financial sector is the largest user of ICT in the world and, according to a study requested by Parliament's Committee on Economic and Monetary Affairs (ECON), there were over 5 100[20] crypto-assets in existence globally in 2020, with a total market capitalization of more than US$250billion. „*The initiative aims to support innovation and fair competition by creating a framework for the issuance, and provision of services related to crypto-assets. In addition, it aims to ensure a high level of consumer and investor protection and market integrity in the crypto-asset markets, as well as address financial stability and monetary policy risks that could arise from a wide use of crypto-assets and DLT-based solutions in financial markets. "*[21]

The Commission was motivated to issue this proposal mainly because some of the member states have already introduced certain rules on crypto-

[15] Ncsl.org. 2021. *Autonomous Vehicles State Bill Tracking Database*. [online] Available at: <https://www.ncsl.org/research/transportation/autonomous-vehicles-legislative-database.aspx> [Accessed 7 November 2021].
[16] Employment (820 ILCS 42/). *Artificial Intelligence Video Interview Act*
[17] Assembly, No. 791, State of New Jersey, 219th Legislature. *An Act establishing creditworthiness guidelines for affordable housing and supplementing Title 46 of the Revised Statutes*.
[18] Jillson, E., 2021. *Aiming for truth, fairness, and equity in your company's use of AI*. [online] Federal Trade Commission. Available at: <https://www.ftc.gov/news-events/blogs/business-blog/2021/04/aiming-truth-fairness-equity-your-companys-use-ai> [Accessed 7 November 2021].
[19] Smith, A., 2020. *Using Artificial Intelligence and Algorithms*. [online] Federal Trade Commission. Available at: <https://www.ftc.gov/news-events/blogs/business-blog/2020/04/using-artificial-intelligence-algorithms> [Accessed 7 November 2021].
[20] Houben, R. and Snyers, A., 2020. Crypto-assets. Key developments, regulatory concerns and responses. [ebook] Brussels: ECON committe. European Parliament. Available at: <https://www.europarl.europa.eu/RegData/etudes/STUD/2020/648779/IPOL_STU(2020)648779_EN.pdf?fbclid=IwAR1QFnOvchhqCbd8-nUOTmwslQRQNmj94z_05ttPJWrSm8fYcpyZVPdYgR8> [Accessed 7 November 2021].
[21] Legislative Train Schedule: The Proposal for a Regulation of the European Parliament and of the Council on markets in cryptoassets, which amends Directive (EU) 2019/1937 (further referred to as „MiCA"). Available at: <https://www.europarl.europa.eu/legislative-train/theme-a-europe-fit-for-the-digital-age/file-crypto-assets-1> [Accessed 7 November 2021]

Ministry of Foreign Affairs of the Czech Republic

The project was supported by the Ministry of Foreign Affairs of the Czech Republic in the framework of public diplomacy projects within Czech foreign policy and international relations

assets, which caused fragmentation of the single market. As a result, it might have led to regulatory arbitrages and it became difficult for crypto-asset service providers to scale – up and expand their cross-border activities. The Commission, therefore, wanted to create a sound, proportionate and comprehensive legal framework, clearly defining the regulatory treatment of all crypto-assets that supports innovation and competition. Another reason was that where crypto-assets are not subject to EU financial regulation, consumers and investors might be exposed to significant risk due to the lack of rules applicable to services related to these assets.

Crypto-assets are in the proposal defined as a digital representation of value or rights, which may be transferred and stored electronically, using distributed ledger technology or similar technology. A primary taxonomy then distinguishes between payment tokens (means of exchange or payment), investment tokens (have profit rights attached), and utility tokens (enable access to a specific product or service). When it comes to MiCA, the European Commission chose a slightly different approach regarding definition. There are no lists and no annexes in this regard. Instead, the definitions are laid quite broadly so as to include possible future developments and changes. The future-proof regulation is therefore not ensured by the delegated acts but rather through broad and versatile definitions. As an example, it may be mentioned that MiCA defines three categories of crypto-assets and those are asset-referenced tokens (ART), e-money tokens (EMT), and a catch-all category called "crypto-assets", encompassing any crypto-asset that is neither an ART nor an EMT (these are often utility tokens or asset tokens). The third category is intentionally defined so widely that it can encompass many different types of crypto-assets, including if some new type emerged. Another difference from AI Act is also in the form of the rules. MiCA contains relatively clear obligations for the issuers rather than performance-based rules. However, those two regulations have in common that MiCA also does not regulate the technology itself but instead regulates it indirectly through the providers or the provided services.

As in the AI Act, it is also possible to find measures for SMEs in MiCA. For example, the issuers of crypto-assets are, according to the regulation, obliged to publish an information document (called white paper) with mandatory disclosure requirements. „*In order to avoid the creation of administrative burden, small and medium-sized enterprises (SMEs) will be exempted from the publication of such an information document where the total consideration of the offering of crypto-assets is less than €1,000,000 over a period of 12 months. Issuers of 'stablecoins' will not be subject to authorisation by a national competent authority (NCA) if the outstanding amount of 'stablecoins' is below €5,000,000. Furthermore, the requirements imposed on crypto-asset service providers are proportionate to the risks created by the services provided."* [22] The costs of whitepaper are estimated at around € 35 000, so it could be devastating for small offerings below the above-specified threshold. [23]

DLT Pilot regime

Proposal for a Regulation on a pilot regime for market infrastructures based on distributed ledger technology („DLT Pilot regime") was introduced together with MiCA and "*aims to provide legal certainty, support innovation, consumer and investor protection and market integrity, and ensure financial stability, by establishing uniform requirements for operating DLT market infrastructures: permissions granted under this Regulation would allow market participants to operate a DLT market infrastructure and to provide their services across all Member States.*" [24] Pilot

[22] Chapter 3 of the Explanatory Memorandum of the MiCA

[23] Zandersone, L., 2021. *Updating the Crypto Assets Regulation and establishing a pilot regime for distributed ledger technology*. [ebook] Brussels. Available at: <https://www.europarl.europa.eu/RegData/etudes/BRIE/2021/662617/EPRS_BRI(2021)662617_EN.pdf> [Accessed 7 November 2021].

[24] Legislative Train Schedule: The Proposal for a Regulation on a pilot regime for market infrastructures based on distributed ledger technology COM/2020/594 final (further referred to as „DLT Pilot regime"). Available at:

Ministry of Foreign Affairs of the Czech Republic

The project was supported by the Ministry of Foreign Affairs of the Czech Republic in the framework of public diplomacy projects within Czech foreign policy and international relations

regime is, as well as MiCA, part of the Digital Finance package – package of measures intended to further enable and support the potential of digital finance in terms of innovation and competition while mitigating associated potential risks. The measures should also help to ensure that existing legislation does not present obstacles to the uptake of new technologies while still reaching the relevant regulatory objectives.

What is unique and interesting about the Pilot regime is that the DLT market infrastructures can request exemptions from specific requirements embedded in EU legislation (MiFID II, CSDR) under this proposal. National competent authorities, that grant the permission to operate the DLT market infrastructure upon fulfilment of requirements to mitigate some risks associated with the use of DLT, are also in charge of granting these exemptions if it complies with the conditions attached to each exemption. To ensure a level playing field across the EU, the requested exemptions (set out in Articles 4 and 5) are limited and might have attached conditions. Therefore, the pilot regime will allow for experimentation within a safe environment and provide evidence for possible further amendments to existing regulations.

Conclusion

To conclude, it is vital that the European Union is very active in digitalization and new technologies because it is an area that will only grow bigger and more important. Furthermore, Europe might take the role of a global "standard" setter and create a regulation of such elaborate and high quality that even foreign countries will voluntarily adopt those systems and produce their products according to European standards. We could see this process also happening with GDPR, which was feared at be beginning by many but is now considered to be one of the best and most robust standards of personal data protection worldwide, which, in rare cases, has been adopted by even non-European countries (for example Serbia adjusted its data protection framework to GDPR).

When regulating new technologies, the EU should follow these key principles. Most importantly, to ensure the appropriate protection of users, businesses, investments, or financial stability. However, there is no need for duplicity of the regulation, so the EU should regulate only areas and issues not addressed by different legislation, which already offer sufficient protection. The rules should furthermore be set out also with regard to small-scale providers like SMEs or star-ups and should not be overly burdensome for them. Reasonable regulation without unnecessary administrative obligations is the key to a booming and safe market. Therefore, the new legislative acts should entail measures in support of innovation like the AI Act and MiCA already do. SMEs and start-ups usually struggle with financing, and compliance with all the relevant regulations could be too costly for them and can prevent them from further development and progress. Especially with the ex-ante regulation, it is essential to ensure that start-ups can put their products on the market as soon as possible and start generating at least some profit. One of the solutions to the problems mentioned above and a tool for innovation-friendly regulation seems to be the implementation of regulatory sandboxes and experimentation clauses. These institutes might be tremendously valuable for placing new innovative products on the market. They provide benefits not only for the providers of such product or service themselves but also for the supervisory authorities that can gain valuable insights into the functioning of the respective technology or product through close cooperation and dialogue with the provider in the sandbox. The Council perceives in its Conclusion regulatory sandboxes „*as concrete frameworks which, by providing a structured context for experimentation, enable where appropriate in a real-world environment the testing of innovative technologies, products, services or approaches – at the moment especially in the context of digitalisation – for a limited time and in a limited part of a sector or area*

<https://www.europarl.europa.eu/legislative-train/theme-a-europe-fit-for-the-digital-age/file-crypto-assets-2/05-2021> [Accessed 7 November 2021]

Ministry of Foreign Affairs of the Czech Republic

The project was supported by the Ministry of Foreign Affairs of the Czech Republic in the framework of public diplomacy projects within Czech foreign policy and international relations

under regulatory supervision ensuring that appropriate safeguards are in place." [25] The legal basis for regulatory sandboxes are then the experimentation clauses[26] used in EU legislation and Member States' legal frameworks.

The business and entrepreneurs should view the EU as an innovation-friendly place that welcomes and supports the initiatives in this field, and motivates the innovative companies to be based in the EU. The consumers then as a place where their data and human rights are duly protected and enjoy a wide range of high-quality technological products and systems.

[25] 2020. Council Conclusions on Regulatory sandboxes and experimentation clauses as tools for an innovation-friendly, future-proof and resilient regulatory framework that masters disruptive challenges in the digital age. [ebook] Brussels: General Secretariat of the Counci. Available at: <https://www.consilium.europa.eu/media/46822/st13026-en20.pdf> [Accessed 7 November 2021].

[26] Defined in the same Conclusion as „Legal provisions which enable the authorities tasked with implementing and enforcing the legislation to exercise on a case-by-case basis a degree of flexibility in relation to testing innovative technologies, products, services or approaches."

Ministry of Foreign Affairs of the Czech Republic

The project was supported by the Ministry of Foreign Affairs of the Czech Republic in the framework of public diplomacy projects within Czech foreign policy and international relations

EUROPEUM
Brussels Office

December
2021

About the author

Michaela Stupková is a legal assistant at the Ministry of Finance of the Czech Republic. She graduated in law from Charles University and specializes in ICT and new technologies law.

Ministry of Foreign Affairs
of the Czech Republic

Co-funded by the
Europe for Citizens Programme
of the European Union

The project was supported by the Ministry of Foreign Affairs of the Czech Republic in the framework of public diplomacy projects within Czech foreign policy and international relations